PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-091456
(43)Date of publication of application : 27.03.2002

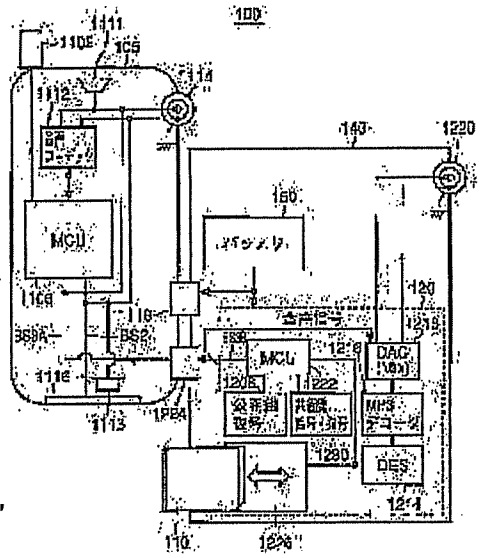
(51)Int.Cl. G10K 15/02
G09C 1/00
G10L 19/00
H04B 7/26
H04L 9/08
H04L 9/32
H04M 1/00
H04M 1/02
H04M 1/725
H04M 11/00

(21)Application number : 2000-285058
(22)Date of filing : 20.09.2000

(71)Applicant : SANYO ELECTRIC CO LTD
(72)Inventor : HORI YOSHIHIRO
OTA SEIYA

(54) PORTABLE TELEPHONE SET AND ADAPTER TO BE USED FOR THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a portable telephone set capable of receiving, decoding, and reproducing enciphered music data without largely changing the constitution of a conventional portable telephone set, and an adapter to be used for the portable telephone set.
SOLUTION: A portable telephone set 100 is constituted of a main body 105 and an adapter 140. The adapter 140 is provided with a data terminal 120, a battery 150, and a jack 1220. The data terminal equipment 120 records the enciphered music data received by the main body 105 in a memory card 110 mounted on an attaching/detaching part 1226. Also, the data terminal equipment 120 reads and decodes the enciphered music data from the memory card 110 by using a public key decoding part 1206, a common key enciphering and decoding part 1230, and a DES 1214. Then, the data terminal equipment 120 defrosts and reproduces the music data by an MP3 decoder 1216, and outputs the music data to a jack 1220.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－91456
（P2002－91456A）
(43)公開日　平成14年３月27日(2002.3.27)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	５Ｋ０２３
Ｇ１０Ｌ　19/00		Ｈ０４Ｍ　1/00	Ｒ	５Ｋ０２７
Ｈ０４Ｂ　7/26		1/02	Ｃ	５Ｋ０６７
Ｈ０４Ｌ　9/08		1/725		５Ｋ１０１

審査請求　未請求　請求項の数19　ＯＬ　（全 28 頁）　最終頁に続く

(21)出願番号　特願2000－285058(P2000－285058)

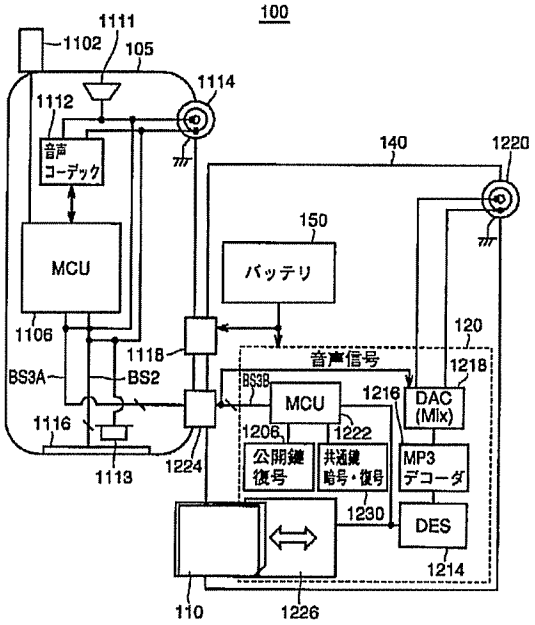
(22)出願日　平成12年９月20日(2000.9.20)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　太田　晴也
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　携帯電話機およびそれに用いるアダプタ

(57)【要約】
【課題】　従来の携帯電話機の構成を大幅に変更することなく、暗号化音楽データの受信、復号および再生を行なうことができる携帯電話機およびそれに用いるアダプタを提供する。
【解決手段】　携帯電話機１００は、本体１０５とアダプタ１４０とから成る。アダプタ１４０は、データ端末装置１２０と、バッテリ１５０と、ジャック１２２０とを含む。データ端末装置１２０は、本体１０５によって受信された暗号化音楽データ等を着脱部１２２６に装着されたメモリカード１１０へ記録する。また、データ端末装置１２０は、公開鍵復号部１２０６、共通鍵暗号・復号部１２３０、およびＤＥＳ１２１４によってメモリカード１１０から暗号化音楽データを読出し、および復号を行なう。そして、データ端末装置１２０は、ＭＰ３デコーダ１２１６によって音楽データを解凍して再生し、ジャック１２２０へ出力する。



1

【特許請求の範囲】

【請求項１】　音楽データを暗号化した暗号化音楽データと、前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から前記暗号化音楽データと前記ライセンス鍵とを取得して前記音楽データを再生する携帯電話機であって、

本体部と、

前記本体部から脱着可能なアダプタとを備え、

前記アダプタは、

前記データ記録装置を脱着する着脱部と、

データ端末装置とを含み、

前記データ端末装置は、

前記データ記録装置とデータの授受を行なうためのインタフェース部と、

前記ライセンス鍵によって前記暗号化音楽データを復号して前記音楽データを復元する復号処理部と、

前記復号処理部にて復元された音楽データから音楽を再生する音楽再生部と、制御部とを含み、

音楽データの再生時、

前記制御部は、前記データ記録装置に記録された前記暗号化音楽データおよび前記ライセンス鍵を前記インタフェース部を介して取得し、その取得した暗号化音楽データおよびライセンス鍵を前記復号処理部に与える、携帯電話機。

【請求項２】　音楽データを暗号化した暗号化音楽データおよび／または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機であって、

本体部と、

アダプタとを備え、

前記アダプタは、

前記データ記録装置を脱着する着脱部と、

データ端末装置とを含み、

前記データ端末装置は、

前記データ記録装置とデータの授受を行なうためのインタフェース部と、

制御部とを含み、

データの受信時、

前記制御部は、前記本体部から前記暗号化音楽データおよび／または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録する、携帯電話機。

【請求項３】　音楽データを暗号化した暗号化音楽データおよび／または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵をデータ記録装置に記録し、または前記データ記録装置に記録された前記暗号化音楽データと前記ライセンス鍵

2

とを取得して前記音楽データを再生する携帯電話機であって、

本体部と、

アダプタ部とを備え、

前記アダプタ部は、

前記データ記録装置を脱着する着脱部と、

データ端末装置とを含み、

前記データ端末装置は、

前記データ記録装置とデータの授受を行なうためのインタフェース部と、

前記データ記録装置に対する認証データを保持する認証データ保持部と、

前記ライセンス鍵によって前記暗号化音楽データを復号する復号処理部と、

制御部とを含み、

データの受信時、

前記制御部は、前記本体部から前記暗号化音楽データおよび／または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録し、

データの再生時、

前記制御部は、前記認証データを前記インタフェース部を介して前記データ記録装置へ送り、前記データ記録装置において前記認証データが認証されることによって前記データ記録装置から送られて来るライセンス鍵および暗号化音楽データを前記復号処理部へ入力する、携帯電話機。

【請求項４】　前記アダプタ部は、前記データ端末装置から出力される音楽データの再生信号を外部出力装置へ出力するための音楽端子をさらに含む、請求項１または請求項３に記載の携帯電話機。

【請求項５】　前記本体部は、通話時に相手側から受取った音声信号を外部へ出力し、音声信号を入力するための音声端子を含む、請求項４に記載の携帯電話機。

【請求項６】　前記音楽端子は、２チャンネルの出力信号を前記外部へ出力する、請求項４または請求項５に記載の携帯電話機。

【請求項７】　前記本体部は、前記データ端末装置から出力される音楽データの再生信号と、通話時に相手側から受取った音声信号とを外部出力装置へ出力し、音声信号を入力するための音楽音声端子を含む、請求項１または請求項３に記載の携帯電話機。

【請求項８】　前記音楽音声端子は、２チャンネルの出力信号を前記外部出力装置へ出力する、請求項７に記載の携帯電話機。

【請求項９】　前記データ端末装置は、

前記データ記録装置から前記ライセンス鍵を取得するための第１のセッション鍵を発生するセッション鍵発生部と、

前記バスに接続され、前記データ記録装置における前記

認証データの認証に基づいて、前記データ記録装置から取得した第２のセッション鍵によって前記第１のセッション鍵を暗号化する暗号処理部とをさらに含み、
前記復号処理部は、
前記バスに接続され、前記第１のセッション鍵によって暗号化された前記ライセンス鍵を復号する第１の復号処理部と、
前記バスに接続され、前記第１の復号処理部において復号された前記ライセンス鍵によって前記暗号化音楽データを復号する第２の復号処理部とから成り、
データの再生時、
前記制御部は、さらに、前記第２のセッション鍵を前記暗号処理部へ与え、前記第１のセッション鍵によって暗号化されたライセンス鍵を前記第１の復号処理部へ与え、前記暗号化音楽データを前記第２の復号処理部へ与える、請求項１から請求項８のいずれか１項に記載の携帯電話機。

【請求項１０】　前記データ端末装置は、
前記バスに接続され、前記認証データに含まれる公開暗号鍵と非対象な秘密復号鍵を保持する鍵保持部と、
前記バスに接続され、前記公開暗号鍵によって暗号化された前記第２のセッション鍵を前記秘密復号鍵によって復号する第３の復号処理部とをさらに含み、
データの再生時、
前記制御部は、さらに、前記公開暗号鍵によって暗号化された前記第２のセッション鍵を前記データ記録装置から受取り、前記第３の復号処理部へ与え、前記第３の復号処理部において復号された第２のセッション鍵を前記暗号処理部へ与える、請求項９に記載の携帯電話機。

【請求項１１】　前記本体部は、前記データ端末装置を駆動する駆動電源を含む、請求項１から請求項１０のいずれか１項に記載の携帯電話機。

【請求項１２】　前記アダプタ部は、前記データ端末装置を駆動する駆動電源をさらに含む、請求項１から請求項１０のいずれか１項に記載の携帯電話機。

【請求項１３】　音楽データを暗号化した暗号化音楽データと、前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から前記暗号化音楽データと前記ライセンス鍵とを取得して前記音楽データを再生する携帯電話機に装着するアダプタであって、前記データ記録装置を脱着する着脱部と、
データ端末装置とを備え、
前記データ端末装置は、
前記データ記録装置とデータの授受を行なうためのインタフェース部と、
前記データ記録装置に対する認証データを保持する認証データ保持部と、
前記ライセンス鍵によって前記暗号化音楽データを復号する復号処理部と、
制御部とを含み、
音楽データの再生時、
前記制御部は、前記認証データを前記インタフェース部を介して前記データ記録装置へ送り、前記データ記録装置において前記認証データが認証されることによって前記データ記録装置から送られてくる前記ライセンス鍵および前記暗号化音楽データを受取り、その受取った暗号化音楽データおよびライセンス鍵を前記復号処理部に与える、アダプタ。

【請求項１４】　音楽データを暗号化した暗号化音楽データおよび／または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機に装着するアダプタであって、
前記データ記録装置を脱着する着脱部と、
データ端末装置とを備え、
前記データ端末装置は、
前記データ記録装置とデータの授受を行なうためのインタフェース部と、
制御部とを含み、
データの受信時、
前記制御部は、前記携帯電話機から前記暗号化音楽データおよび／または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録する、アダプタ。

【請求項１５】　音楽データを暗号化した暗号化音楽データおよび／または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵とを受信してデータ記録装置に記録し、または前記データ記録装置に記録された前記暗号化音楽データと前記ライセンス鍵とを取得して前記データを再生する携帯電話機に装着するアダプタであって、
前記データ記録装置を着脱するための着脱部と、
データ端末装置とを備え、
前記データ端末装置は、
前記データ記録装置とデータの授受を行なうためのインタフェース部と、
前記データ記録装置に対する認証データを保持する認証データ保持部と、
前記ライセンス鍵によって前記暗号化音楽データを復号する復号処理部と、
制御部とを含み、
データの受信時、
前記制御部は、前記携帯電話機から前記暗号化音楽データおよび／または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録し、
データの再生時、

前記制御部は、前記認証データを前記インタフェース部を介して前記データ記録装置へ送り、前記データ記録装置において前記認証データが認証されることによって前記データ記録装置から送られてくる前記ライセンス鍵および前記暗号化音楽データを受取り、その受取ったライセンス鍵および暗号化音楽データを前記復号処理部へ入力する、アダプタ。

【請求項１６】　前記データ端末装置から出力される音楽データの再生信号を外部出力装置へ出力するための音楽端子をさらに含む、請求項１３または請求項１５に記載のアダプタ。

【請求項１７】　前記データ端末装置の駆動電源をさらに備える、請求項１１３から請求項１６のいずれか１項に記載のアダプタ。

【請求項１８】　前記携帯電話機に対して駆動電源を供給する、請求項１７に記載のアダプタ。

【請求項１９】　前記携帯電話機から駆動電源の供給を受ける、請求項１３から請求項１６のいずれか１項に記載のアダプタ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられる携帯電話機およびそれに用いられるアダプタに関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリに記録する。

【００１２】

【発明が解決しようとする課題】しかし、暗号化音楽コンテンツデータを配信サーバから受信し、その受信した暗号化音楽データを記録したり、復号および再生するためには、従来の携帯電話機における通常の電話機能の他

にメモリカードを制御し、メモリカードからの暗号化音楽コンテンツデータを復号し、かつ、再生するための専用回路が必要であるため、従来の携帯電話機をそのまま用いて受信した暗号化音楽コンテンツデータを記録し、その記録された暗号化音楽コンテンツデータを復号および再生することはできない。

【００１３】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、従来の携帯電話機の構成を大幅に変更することなく、受信した暗号化音楽コンテンツデータを記録し、その記録された暗号化コンテンツデータを復号および再生を行なうことができる携帯電話機およびそれに用いるアダプタを提供することである。

【００１４】

【課題を解決するための手段および発明の効果】この発明による携帯電話機は、音楽データを暗号化した暗号化音楽データと、暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から暗号化音楽データとライセンス鍵とを取得して音楽データを再生する携帯電話機であって、本体部と、本体部から脱着可能なアダプタとを備え、アダプタは、データ記録装置を脱着する着脱部と、データ端末装置とを含み、データ端末装置は、データ記録装置とデータの授受を行なうためのインタフェース部と、ライセンス鍵によって暗号化音楽データを復号して音楽データを復元する復号処理部と、復号処理部にて復元された音楽データから音楽を再生する音楽再生部と、制御部とを含み、音楽データの再生時、制御部は、データ記録装置に記録された暗号化音楽データおよびライセンス鍵をインタフェース部を介して取得し、その取得した暗号化音楽データおよびライセンス鍵を前記復号処理部に与える。

【００１５】この発明による携帯電話機においては、暗号化音楽データとライセンス鍵とが記録されたデータ記録装置がアダプタに装着された状態で、アダプタに含まれるデータ端末装置は、データ記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【００１６】したがって、この発明によれば、暗号化音楽データの再生を、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、データ端末装置が含まれるアダプタを新規に装着するだけで携帯電話機の本体の構成を殆ど変更せずに暗号化音楽データの再生が可能である。

【００１７】また、この発明による携帯電話機は、音楽データを暗号化した暗号化音楽データおよび／または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機であって、本体部と、アダプタとを備え、アダプタは、データ記録装置を脱着する着脱部と、データ端末装置とを含み、データ端末装置は、データ記録装置とデータの授受を行なうためのインタフェース部と、制御部とを含み、データの受信時、制御部は、本体部から暗号化音楽データおよび／またはライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵をインタフェース部を介してデータ記録装置に記録する。

【００１８】この発明による携帯電話機においては、アダプタにデータ記録装置が装着された状態で、暗号化音楽データおよびライセンス鍵が本体側で受信され、アダプタ部のデータ端末装置へ送られる。そして、データ端末装置は、送られてきた暗号化音楽データとライセンス鍵とをデータ記録装置に記録する。

【００１９】したがって、この発明によれば、暗号化音楽データのダウンロードを、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、データ端末装置が含まれるアダプタを新規に装着するだけで携帯電話機の本体の構成を殆ど変更せずに暗号化音楽データのダウンロードが可能である。

【００２０】また、この発明による携帯電話機は、音楽データを暗号化した暗号化音楽データおよび／または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵をデータ記録装置に記録し、またはデータ記録装置に記録された暗号化音楽データとライセンス鍵とを取得して音楽データを再生する携帯電話機であって、本体部と、アダプタ部とを備え、アダプタ部は、データ記録装置を脱着する着脱部と、データ端末装置とを含み、データ端末装置は、データ記録装置とデータの授受を行なうためのインタフェース部と、データ記録装置に対する認証データを保持する認証データ保持部と、ライセンス鍵によって暗号化音楽データを復号する復号処理部と、制御部とを含み、データの受信時、制御部は、本体部から暗号化音楽データおよび／またはライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵をインタフェース部を介してデータ記録装置に記録し、データの再生時、制御部は、認証データをインタフェース部を介してデータ記録装置へ送り、データ記録装置において認証データが認証されることによってデータ記録装置から送られて来るライセンス鍵および暗号化音楽データを復号処理部へ入力する。

【００２１】この発明による携帯電話機においては、アダプタにデータ記録装置が装着された状態で、暗号化音楽データおよびライセンス鍵が本体側で受信され、アダプタ部のデータ端末装置へ送られる。そして、データ端末装置は、送られてきた暗号化音楽データとライセンス鍵とをデータ記録装置に送る。データ記録装置は暗号化音楽データとライセンス鍵とを記録する。また、アダプタ部に含まれるデータ端末装置は、音楽データの再生時、データ記録装置に対する認証が終了した後にデータ

記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【００２２】したがって、この発明によれば、暗号化音楽データのダウンロード、およびダウンロードした暗号化音楽データの再生を、携帯電話機のアダプタ部にデータ記録装置を装着して行なうことができる。その結果、データ端末装置が含まれるアダプタを新規に装着するだけで携帯電話機の本体の構成を殆ど変更せずに暗号化音楽データのダウンロード、およびダウンロードした暗号化音楽データの再生が可能である。

【００２３】好ましくは、携帯電話機のアダプタ部は、データ端末装置から出力される音楽データの再生信号を外部出力装置へ出力するための音楽端子をさらに含む。

【００２４】アダプタ部に含まれるデータ端末装置によって暗号化音楽データが復号、および再生されると、その再生された音楽データはアダプタに設けられた音楽端子に送られる。そして、音楽端子を介してヘッドホン等の外部出力装置へ音楽データが出力される。

【００２５】したがって、この発明によれば、携帯電話機の本体に音楽データ専用の端子を新たに設けずにダウンロードした音楽を聴くことができる。

【００２６】好ましくは、携帯電話機の本体部は、通話時に相手側から受取った音声信号を外部へ出力し、音声信号を入力するための音声端子を含む。

【００２７】携帯電話機の本体側で受取られた相手側の音声信号は復調等されて本体に設けられた音声端子から外部へ出力される。また、アダプタ部に含まれるデータ端末装置によって復号および再生された音楽データはアダプタ部に設けられた音楽データ専用の音楽端子から外部へ出力される。

【００２８】したがって、この発明によれば、従来の携帯電話機の構成を殆ど変更せずに、データ端末装置を含むアダプタを装着するだけでダウンロードされた音楽を専用端子から聴くことができる。

【００２９】好ましくは、アダプタ部に設けられた音楽端子は、２チャンネルの出力信号を外部へ出力する。

【００３０】音楽データ専用の音楽端子は、データ端末装置によって復号および再生された音楽データを２チャンネルの信号としてヘッドホン等の外部出力装置へ出力する。

【００３１】したがって、携帯電話機のユーザは、ダウンロードした音楽をステレオによって聴くことができる。

【００３２】好ましくは、携帯電話機の本体部は、データ端末装置から出力される音楽データの再生信号と、通話時に相手側から受取った音声信号とを外部出力装置へ出力し、音声信号を入力するための音楽音声端子を含む。

【００３３】携帯電話機によって受信された音声信号、およびデータ端末装置によって再生された音楽データは、本体に設けられた音楽音声端子を介して外部出力装置へ出力される。また、携帯電話機のユーザが話した音声信号は、音楽音声端子から携帯電話機へ取込まれ、相手側へ送信される。つまり、１つの端子を介して通常の通話、および音楽の再生が行なわれる。

【００３４】したがって、この発明によれば、音楽を聴きながら通常の通話を行なうことができる。

【００３５】好ましくは、携帯電話機の本体に設けられた音楽音声端子は、２チャンネルの出力信号を外部出力装置へ出力する。

【００３６】携帯電話機の本体は、１つの端子を介して音声信号の入出力および音楽データの出力を行なう。そして、携帯電話機の本体は、音楽データを２チャンネルの出力信号としてヘッドホン等の外部出力装置へ出力する。

【００３７】したがって、この発明によれば、ステレオで音楽を聴きながら通常の通話を行なうことができる。

【００３８】好ましくは、携帯電話機のアダプタ部に含まれるデータ端末装置は、データ記録装置からライセンス鍵を取得するための第１のセッション鍵を発生するセッション鍵発生部と、バスに接続され、データ記録装置における認証データの認証に基づいて、データ記録装置から取得した第２のセッション鍵によって第１のセッション鍵を暗号化する暗号処理部とをさらに含み、復号処理部は、バスに接続され、第１のセッション鍵によって暗号化されたライセンス鍵を復号する第１の復号処理部と、バスに接続され、第１の復号処理部において復号されたライセンス鍵によって暗号化音楽データを復号する第２の復号処理部とから成り、データの再生時、制御部は、さらに、第２のセッション鍵を暗号処理部へ与え、第１のセッション鍵によって暗号化されたライセンス鍵を第１の復号処理部へ与え、暗号化音楽データを第２の復号処理部へ与える。

【００３９】暗号化音楽データの再生時、データ端末装置は、データ端末装置に対する認証が終了した後、データ端末装置とデータ記録装置とにおいて発生されたセッション鍵によってデータ記録装置との間で相互認証を行ないながら、データ記録装置から暗号化音楽データおよびライセンス鍵を受取る。そして、データ端末装置は、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【００４０】したがって、この発明によれば、暗号化音楽データを正規のデータ端末装置によって再生することができる。その結果、携帯電話機を用いて暗号化音楽データを保護しながら音楽を楽しむことができる。

【００４１】好ましくは、携帯電話機のアダプタ部に含まれるデータ端末装置は、バスに接続され、認証データに含まれる公開暗号鍵と非対象な秘密復号鍵を保持する鍵保持部と、バスに接続され、公開暗号鍵によって暗号

化された第２のセッション鍵を秘密復号鍵によって復号する第３の復号処理部とをさらに含み、データの再生時、制御部は、さらに、公開暗号鍵によって暗号化された第２のセッション鍵をデータ記録装置から受取り、第３の復号処理部へ与え、第３の復号処理部において復号された第２のセッション鍵を暗号処理部へ与える。

【００４２】データ端末装置は、音楽データの再生時、公開鍵方式によってデータ記録装置において発生された第２のセッション鍵を受取る。そして、データ端末装置は、受取った第２のセッション鍵によって、自己が発生させた第１のセッション鍵を暗号化してデータ記録装置へ送り、第１のセッション鍵によって暗号化されたライセンス鍵をデータ記録装置から受取る。

【００４３】したがって、この発明によれば、データ端末装置は秘密復号鍵を保持していれば良く、暗号化したデータのやり取りにおける鍵の管理が容易になる。また、この発明によれば、認証データによるデータ端末装置のデータ記録装置に対する認証、およびセッション鍵によるデータ端末装置とデータ記録装置との相互認証という２重のセキュリティによって暗号化音楽データを保護できる。

【００４４】好ましくは、携帯電話機の本体部は、アダプタ部に含まれるデータ端末装置を駆動する駆動電源を含む。

【００４５】携帯電話機に備えられた駆動電源からデータ端末装置を駆動するための駆動電力が供給される。したがって、この発明によれば、データ端末装置を含むアダプタのみを装着することによって従来の携帯電話機の構成を殆ど変更せずに暗号化音楽データをダウンロードでき、そのダウンロードした暗号化音楽データを復号および再生できる。

【００４６】好ましくは、アダプタ部は、データ端末装置を駆動する駆動電源をさらに含む。

【００４７】アダプタ部に含まれるデータ端末装置は、アダプタ部に含まれる駆動電源によって駆動され、暗号化音楽データの再生等を行なう。したがって、この発明によれば、暗号化音楽データのダウンロード、および復号・再生を行なうための電力と携帯電話機の本体を駆動するための電力とを賄なう駆動電源をアダプタ部に設けることによって、従来の携帯電話機の構成を殆ど変更せずに暗号化音楽データのダウンロード、および復号・再生を行なうことができる。

【００４８】また、この発明によるアダプタは、音楽データを暗号化した暗号化音楽データと、暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から暗号化音楽データとライセンス鍵とを取得して音楽データを再生する携帯電話機に装着するアダプタであって、データ記録装置を脱着する着脱部と、データ端末装置とを備え、データ端末装置は、データ記録装置とデータの授受を行なうためのインタフェース部と、データ記録装置に対する認証データを保持する認証データ保持部と、ライセンス鍵によって暗号化音楽データを復号する復号処理部と、制御部とを含み、音楽データの再生時、制御部は、認証データをインタフェース部を介してデータ記録装置へ送り、データ記録装置において認証データが認証されることによってデータ記録装置から送られてくるライセンス鍵および暗号化音楽データを受取り、その受取った暗号化音楽データおよびライセンス鍵を復号処理部に与える。

【００４９】この発明によるアダプタにおいては、暗号化音楽データおよびライセンス鍵が記録されたデータ記録装置が装着された状態で、アダプタに含まれるデータ端末装置は、データ記録装置に対する認証が終了した後にデータ記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【００５０】したがって、この発明によれば、暗号化音楽データの再生を携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、携帯電話機のユーザは、データ端末装置が含まれるアダプタを新規に購入するだけで、携帯電話機を用いて暗号化音楽データの再生を行なうことができる。

【００５１】また、この発明によるアダプタは、音楽データを暗号化した暗号化音楽データおよび／または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機に装着するアダプタであって、データ記録装置を脱着する着脱部と、データ端末装置とを備え、データ端末装置は、データ記録装置とデータの授受を行なうためのインタフェース部と、制御部とを含み、データの受信時、制御部は、携帯電話機から暗号化音楽データおよび／またはライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵をインタフェース部を介してデータ記録装置に記録する。

【００５２】この発明によるアダプタにおいては、データ記録装置が装着された状態で、携帯電話機の本体側で受信され暗号化音楽データおよびライセンス鍵が入力される。そして、アダプタに含まれるデータ端末装置は、入力された暗号化音楽データとライセンス鍵とをデータ記録装置に送る。データ記録装置は暗号化音楽データとライセンス鍵とを記録する。

【００５３】したがって、この発明によれば、暗号化音楽データのダウンロードを、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、携帯電話機のユーザは、データ端末装置が含まれるアダプタを新規に購入するだけで、携帯電話機を用いて暗号化音楽データのダウンロードを行なうことができる。

【００５４】また、この発明によるアダプタは、音楽デ

ータを暗号化した暗号化音楽データおよび／または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵とを受信してデータ記録装置に記録し、またはデータ記録装置に記録された暗号化音楽データとライセンス鍵とを取得してデータを再生する携帯電話機に装着するアダプタであって、データ記録装置を着脱するための着脱部と、データ端末装置とを備え、データ端末装置は、データ記録装置とデータの授受を行なうためのインタフェース部と、データ記録装置に対する認証データを保持する認証データ保持部と、ライセンス鍵によって暗号化音楽データを復号する復号処理部と、制御部とを含み、データの受信時、制御部は、携帯電話機から暗号化音楽データおよび／またはライセンス鍵を受取り、その受取った暗号化音楽データおよび／またはライセンス鍵をインタフェース部を介してデータ記録装置に記録し、データの再生時、制御部は、認証データをインタフェース部を介してデータ記録装置へ送り、データ記録装置において認証データが認証されることによってデータ記録装置から送られてくるライセンス鍵および暗号化音楽データを受取り、その受取ったライセンス鍵および暗号化音楽データを復号処理部へ入力する。

【００５５】この発明によるアダプタにおいては、データ記録装置が装着された状態で、携帯電話機の本体側で受信され暗号化音楽データおよびライセンス鍵が入力される。そして、アダプタに含まれるデータ端末装置は、入力された暗号化音楽データとライセンス鍵とをデータ記録装置に送る。データ記録装置は暗号化音楽データとライセンス鍵とを記録する。また、アダプタに含まれるデータ端末装置は、音楽データの再生時、データ記録装置に対する認証が終了した後にデータ記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【００５６】したがって、この発明によれば、暗号化音楽データのダウンロード、およびダウンロードした暗号化音楽データの再生を、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、携帯電話機のユーザは、データ端末装置が含まれるアダプタを新規に購入するだけで、携帯電話機を用いて暗号化音楽データのダウンロードし、かつ、ダウンロードした暗号化音楽データの再生を行なうことができる。

【００５７】好ましくは、アダプタは、データ端末装置から出力される音楽データの再生信号を外部出力装置へ出力するための音楽端子をさらに含む。

【００５８】アダプタに含まれるデータ端末装置によって暗号化音楽データが復号、および再生されると、その再生された音楽データはアダプタに設けられた音楽端子に送られる。そして、音楽端子を介してヘッドホン等の外部出力装置へ音楽データが出力される。

【００５９】したがって、この発明によれば、携帯電話機の本体に音楽データ専用の端子を新たに設けずにダウンロードした音楽を聴くことができる。

【００６０】好ましくは、アダプタはデータ端末装置の駆動電源をさらに備える。アダプタに含まれるデータ端末装置は、アダプタに含まれる駆動電源によって駆動され、暗号化音楽データの再生等を行なう。したがって、この発明によれば、暗号化音楽データのダウンロード、および復号・再生を行なうための電力と携帯電話機の本体を駆動するための電力とを賄なう駆動電源をアダプタに設けることによって、従来の携帯電話機の構成を殆ど変更せずに暗号化音楽データのダウンロード、および復号・再生を行なうことができる。

【００６１】好ましくは、アダプタは携帯電話機に対して駆動電源を供給する。アダプタは、通常の電話機能を果たす携帯電話機に駆動電源を供給する。

【００６２】したがって、この発明によれば、従来の電話機能を果たす携帯電話機にアダプタを装着することによって暗号化音楽データを再生することができる。

【００６３】好ましくは、アダプタは、携帯電話機から駆動電源の供給を受ける。アダプタは、装着された携帯電話機から駆動電源の供給を受け、暗号化音楽データを再生する。

【００６４】したがって、この発明によれば、従来の携帯電話機にアダプタを装着するだけで暗号化音楽データを再生することができる。

【００６５】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００６６】［実施の形態１］図１は、本発明による携帯電話機が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００６７】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【００６８】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセ

ンスとを配信する。

【００６９】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱な可能なメモリカード１１０が装着される。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機１００中の音楽再生回路（図示せず）に与える。

【００７０】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００７１】以下では、このようなライセンスサーバ１０と配信キャリア２０と併せて、配信サーバ３０と総称することにする。

【００７２】また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００７３】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００７４】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００７５】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００７６】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置および音楽再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００７７】図２を参照して、この発明による携帯電話機１００の外観について説明する。図２は、携帯電話機１００の裏面を示したものである。携帯電話機１００は、アダプタ１４０と、結合端子１１１８，１２２４とを含む。アダプタ１４０は、メモリカード１１０を着脱するための着脱部１２２６と、暗号化音楽データを復号および再生して聴くためのヘッドホン１３０を接続するためのジャック１２２０とを備える。結合端子１１１８，１２２４は、携帯電話機１００の本体１０５とアダプタ１４０とを接続する。したがって、後述するように、配信サーバ３０からの暗号化音楽データの配信においては、結合端子１２２４を介して、暗号化音楽データ等がやり取りされる。また、後述するようにアダプタ１４０はバッテリを含むため、携帯電話機１００の本体１０５の駆動用電力は結合端子１１１８を介して本体１０５へ供給される。

【００７８】さらに、アダプタ１４０は本体１０５から着脱可能であり、すでに販売されている携帯電話機に駆動電力を供給するバッテリアダプタを交換して装着可能な構造になっている。したがって、メモリカード１１０の着脱部１２２６、および後述する暗号化音楽データを復号・再生するための機能を必要とするユーザのみが、アダプタ１４０だけを購入して、自己の携帯電話機にアダプタ１４０を装着すれば、配信サーバ３０から希望する暗号化音楽データをダウンロードし、かつ、暗号化音楽データを復号・再生できる。

【００７９】図３を参照して、携帯電話機１００は、本体１０５と、アダプタ１４０とから成る。本体１０５は、アンテナ１１０２と、マイクロコンピュータユニット（ＭＣＵ）１１０６と、音声コーデック１１１２と、スピーカ１１１１と、マイク１１１３と、ジャック１１１４と、バッド１１１６とを含む。ＭＣＵ１１０６は、データバスＢＳ２を介してバッド１１１６と接続される。また、ＭＣＵ１１０６は、データバスＢＳ２と独立なデータバスＢＳ３Ａおよび結合端子１２２４を介してアダプタ１４０に接続される。

【００８０】アンテナ１１０２は、通常の電話機能においては、相手側の音声信号を受信し、その受信した音声信号をＭＣＵ１１０６へ与える。また、携帯電話機１００のユーザが話した音声信号を相手の電話へ送信する。また、アンテナ１１０２は、配信サーバ３０から暗号化音楽データをダウンロードするときは、配信サーバ３０との間でデータを送受信する。

【００８１】ＭＣＵ１１０６は、携帯電話機１００の通常の電話機能等を制御する。音声コーデック１１１２は、通常の電話機能において相手側の音声信号をＭＣＵ１１０６から受取り、その受取った音声信号を復調し、ディジタル信号からアナログ信号へ変換してスピーカ１１１１またはジャック１１１４へ出力し、データバスＢＳ２を介してバッド１１１６へ、さらにデータバスＢＳ３Ａと結合端子１２２４を介してアダプタ１４０へ出力する。また、音声コーデック１１１２は、携帯電話機１００のユーザが話した音声データをマイク１１１３、ジャック１１１４またはデータバスＢＳ２を介してバッド１１１６から受取り、その受取った音声データをアナロ

グ信号からディジタル信号へ変換し、所定の方式に変調してＭＣＵ１１０６へ与える。

【００８２】ジャック１１１４は、イヤホンマイク（図示せず）に接続可能な端子であり、音声コーデック１１１２によって復調等された音声データをイヤホンマイクへ出力する。また、ジャック１１１４は、携帯電話機１００のユーザが話した音声データをイヤホンマイクを介して受取り、音声コーデック１１１２へ出力する。なお、ジャック１１１４は、モノラルの音声データを出力する。

【００８３】バッド１１１６は、外部インタフェースと内部インタフェースとを含み、外部からの制御コマンドを外部インタフェースを介して内部インタフェースへ引込む。また、バッド１１１６はマイク（図示せず）またはイヤホン（図示せず）と接続され、音声コーデック１１１２によって復調等された音声データをデータバスＢＳ２を介して受取り、バッド１１１６を介してイヤホンへ出力するとともに、携帯電話機１００のユーザが話した音声データをバッド１１１６を介して、マイクから受取り、バスＢＳ２を介して音声コーデック１１１２へ出力する。

【００８４】アダプタ１４０は、データ端末装置１２０と、バッテリ１５０と、ジャック１２２０とを含む。バッテリ１５０は、データ端末装置１２０へ駆動電力を供給するとともに、本体１０５へ結合端子１１１８を介して駆動電力を供給する。バッテリ１５０は、メモリカード１１０から暗号化音楽データを読出して復号および再生を行なうデータ端末装置１２０を駆動するための電源、および本体１０５のＭＣＵ１１０６等を駆動するための電源として機能するため、アダプタ１４０に含まれる。すなわち、バッテリ１５０は、メモリカード１１０からの暗号化音楽データの読出し、復号、および再生という特殊機能を有するデータ端末装置１２０も含め、携帯電話機１００全体の駆動電力を供給する必要があるため、アダプタ１４０に新設したものである。これによって、ユーザはアダプタ１４０のみを購入して、携帯電話機のバッテリアダプタと交換して装着できる。その結果、ユーザは、メモリカード１１０への暗号化音楽データのダウンロードおよび復号・再生を容易に行なうことができる。

【００８５】ジャック１２２０は、本体１０５の音声コーデック１１１２によって復調等された音声データをデータ端末装置１２０を介して受取り、接続されたヘッドホン１３０へ出力する。また、ジャック１２２０は、データ端末装置１２０によって復号および再生された音楽データを接続されたヘッドホン１３０へ出力する。なお、ジャック１２２０は、２チャネルの音声データを出力する。

【００８６】データ端末装置１２０は、公開鍵復号部１２０６と、ＤＥＳ１２１４と、ＭＰ３デコーダ１２１６と、ＤＡＣ１２１８と、ＭＣＵ１２２２と、共通鍵暗号・復号部１２３０とを含む。データバスＢＳ３Ｂは、結合端子１２２４を介して本体１０５のデータバスＢＳ３Ａと接続される。すなわち、本体１０５のＭＰＵ１１０６とアダプタ１４０のＭＰＵは、データバスＢＳ３Ａ、結合端子１２２４およびデータバスＢＳ３Ｂを介して接続される。以降、結合端子１２２４で接続されたデータバスＢＳ３ＡおよびデータバスＢＳ３Ｂを総称してデータバスＢＳ３と称する。

【００８７】ＭＣＵ１２２２は、配信サーバ３０からの暗号化音楽データの配信時、着脱部１２２６に装着されたメモリカード１１０からのデータ等を結合端子１２２４およびバスＢＳ３を介して本体１０５のＭＣＵへ出力するとともに、本体１０５のＭＣＵ１１０６からのデータ等をメモリインタフェースを介してメモリカード１１０へ出力する。

【００８８】また、ＭＣＵ１２２２はメモリカード１１０からの暗号化音楽データを復号および再生するとき、メモリカード１１０からのデータ等を公開鍵復号部１２０６、共通鍵暗号・復号部１２３０へ入出力するとともに、暗号化音楽データと、その暗号化音楽データを復号するためのライセンス鍵をＤＥＳ１２１４へ与える。

【００８９】公開鍵復号部１２０６は、後述するように公開鍵による復号処理を行なう。共通鍵暗号・復号部１２３０は、後述するように共通鍵による暗号処理および復号処理を行なう。

【００９０】ＤＥＳ１２１４は、ライセンス鍵によって暗号化音楽データを復号する。ＭＰ３デコーダ１２１６は、ＭＰ３（ＭＰＥＧ１オーディオ・レイヤ３）方式によって圧縮された音楽データを解凍して再生する。

【００９１】ＤＡＣ１２１８は、ＭＰ３デコーダ１２１６によって解凍して再生された音楽データをディジタル信号からアナログ信号へ変換する。

【００９２】上述したようにアダプタ１４０は、配信サーバ３０からダウンロードした暗号化音楽データを記録するためにメモリカード１１０へ与え、暗号化音楽データをメモリカード１１０から読出して復号および再生するためのデータ端末装置１２０と、データ端末装置１２０と、本体１０５の各部とに電力を供給するバッテリ１５０を含む。

【００９３】以下、携帯電話機１００を用いた配信サーバ３０からの暗号化音楽データの配信、およびその配信された暗号化音楽データの復号・再生について説明する。

【００９４】図４は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。ここでは、ＭＰ３方式によって符号化された音楽データを再生するための構成を示しているが、音楽データの圧縮方式を規定するものではなく、他の符号化方式によって符号化された音楽データに

いてはＭＰ３デコーダ１２１６に代えて、音楽データを符号化した復号化方式に適したデコーダを配置すれば実現可能である。

【００９５】まず、配信サーバ３０より配信されるデータについて説明する。携帯電話機１００に配信されるべきＤａｔａは、ＭＰ３方式によって符号化された音楽データから成るコンテンツデータである。コンテンツデータＤａｔａには、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

【００９６】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００９７】さらに、配信サーバ３０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、ライセンス情報としては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）のアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１およびデータ端末装置（携帯電話機またはアダプタ）における制御情報である再生回路制御情報ＡＣ２等が存在する。以後、ライセンス鍵ＫｃとコンテンツＩＤとライセンスＩＤとアクセス制御情報ＡＣ１と再生回路制御情報ＡＣ２とを併せて、ライセンスと総称することとする。

【００９８】図５は、図１に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【００９９】本発明の実施の形態１においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【０１００】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止されるデータ端末装置およびメモリカードのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。

【０１０１】禁止クラスリストデータＣＲＬは、配信サーバ３０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データＣＲＬ＿ｄａｔを配信サーバ３０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬが書替えられる構成とする。また、禁止クラスリストのバージョンについては、ＣＲＬ＿ｖｅｒをメモリカード側より出力し、これを配信サーバ３０側で確認することによってバージョン管理を実行する。差分データＣＲＬ＿ｄａｔには新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【０１０２】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカード内でおいても保持運用することによって、クラス固有すなわち、データ端末装置およびメモリカードの種類に固有の復号鍵が破られた、データ端末装置およびメモリカードへのライセンス鍵の供給が禁止される。このため、データ端末装置ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【０１０３】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリ回路内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【０１０４】データ端末装置およびメモリカードには固有の公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉがそれぞれ設けられ、公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉは携帯電話機に固有の秘密復号鍵Ｋｐｎおよびメモリカード固有の秘密復号鍵Ｋｍｃｉによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、データ端末装置の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【０１０５】また、暗号化音楽データを再生するデータ端末装置およびメモリカードのクラス証明書として、ＣｒｔｆｎおよびＣｍｃｉがそれぞれ設けられる。

【０１０６】これらのクラス証明書は、データ端末装置およびメモリカードのクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【０１０７】これらのコンテンツ再生装置およびメモリカードのクラス固有の公開暗号鍵およびクラス証明書

は、認証データ｛ＫＰｐｎ／／Ｃｒｔｆｎ｝ＫＰｍａおよび｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａの形式で、出荷時にデータ端末装置を搭載した携帯電話機およびメモリカードにそれぞれ記録される。また、データ端末装置１２０を含むアダプタ１４０を単独で出荷する場合は、証明書は上記の認証データの形式で出荷時にアダプタ１４０のデータ端末装置１２０に記録される。後ほど詳細に説明するが、ＫＰｍａは配信システム全体で共通の公開認証鍵である。

【０１０８】図６は、図１に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【０１０９】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ３０、データ端末装置１２０、メモリカード１１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【０１１０】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、データ端末装置もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【０１１１】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、データ端末装置およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、データ端末装置において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【０１１２】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍと、公開暗号鍵ＫＰｍで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍが存在する。

【０１１３】図７は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。

【０１１４】ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４、課金データベース３０２およびＣＲＬデータベース３０６からのデータをデータバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【０１１５】データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードから携帯電話機を介して送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを通信装置３５０およびデータバスＢＳ１を介して受けて、公開認証鍵ＫＰｍａによる復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｍを用いて暗号化して、データバスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをデータバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【０１１６】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよび再生回路制御情報ＡＣ２を、復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してデータバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【０１１７】ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１１８】図８は、図３に示した携帯電話機１００の本体１０５の構成をさらに詳細に説明するための概略ブロック図である。

【０１１９】携帯電話機１００の本体１０５は、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、外部からの指示を携帯電話機１００に与えるためのキー操作部１１０８と、ＭＣＵ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０とを、図３の構成に追加して含む。

【０１２０】なお、図８においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一

部記載を省略している。

【０１２１】図９は、図３に示したデータ端末装置１２０の概略ブロックを詳細に示したものである。データ端末装置１２０は、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ３との間のデータの授受を制御するためのメモリインタフェース１２００とをさらに含む。

【０１２２】データ端末装置１２０は、また、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｒｔｆ１を公開復号鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを保持する認証データ保持部１２０２をさらに含む。ここで、携帯電話機（コンテンツ再生回路）１００のクラスｎは、ｎ＝１であるとする。

【０１２３】データ端末装置１２０は、さらに、データ端末装置に固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１２０４と、データバスＢＳ３から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１２０５とをさらに含む。Ｋｐ１保持部１２０４と復号処理部１２０５とは図３に示す公開鍵復号部１２０６に相当する。

【０１２４】データ端末装置１２０は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でデータバスＢＳ３上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１２１０と、生成されたセッションキーＫｓ３を復号処理部１２０５によって得られたセッションキーＫｓ２によって暗号化し、データバスＢＳ３に出力する暗号化処理部１２０８とを含む。

【０１２５】データ端末装置１２０は、さらに、データバスＢＳ３上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１２１２とを含む。暗号処理部１２０８、セッションキー発生部１２１０、および復号処理部１２１２は、図３に示す共通鍵暗号・復号部１２３０に相当する。

【０１２６】データ端末装置１２０は、さらに、データバスＢＳ３より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１２１２からバスＢＳ３を介して取得したライセンス鍵Ｋｃによって復号し、コンテンツデータを出力する復号処理部１２１４と、復号処理部１２１４の出力を受けてコンテンツデータを解凍して再生するためのＭＰ３デコーダ１２１６と、ＭＰ３デコーダ１２１６の出力をディジタル信号からアナログ信号に変換するとともに、携帯電話機１００の本体１０５からバスＢＳ３を介して入力された音声データをミックスするＤＡＣ１２１８とを含む。

【０１２７】図１０は、メモリカード１１０の構成を説明するための概略ブロック図である。

【０１２８】既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃｉおよびＫｍｃｉが設けられ、メモリカードのクラス証明書Ｃｍｃｉが設けられるが、メモリカード１１０においては、これらは自然数ｉ＝１でそれぞれ表わされるものとする。

【０１２９】したがって、メモリカード１１０は、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ１を保持するＫｍｃ保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Ｋｍ１を保持するＫｍ１保持部１４２１と、Ｋｍ１によって復号可能な公開暗号鍵ＫＰｍ１を保持するＫＰｍ１保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵ＫＰｍｃ1およびクラス証明書Ｃｍｃ１を公開認証鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａとして保持する。

【０１３０】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータやライセンスの管理をメモリカード単位で実行することが可能になる。

【０１３１】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０１を介して授受するデータバスＢＳ４と、データバスＢＳ４にメモリインタフェース１２００から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵ＫｍｃｌをＫｍｃ１保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４０４と、ＫＰｍａ保持部１４１４から認証鍵ＫＰｍａを受けて、データバスＢＳ４に与えられるデータからＫＰｍａによる復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してデータバスＢＳ４に出力する暗号化処理部１４０６とを含む。

【０１３２】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｎもしくは他のメモリカードの公開暗号鍵ＫＰｍｃｉによって暗号化してデータバスＢＳ４に送出する暗号化

処理部１４１０と、データバスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号し、復号結果をデータバスＢＳ５に送出する復号処理部１４１２とを含む。

【０１３３】メモリカード１１０は、さらに、データバスＢＳ４上のデータを公開暗号鍵ＫＰｍ１と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号するための復号処理部１４２２と、禁止クラスリストのバージョン更新のためのデータＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬをデータバスＢＳ５より受けて格納するとともに、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをデータバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。

【０１３４】メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスを保持するためのライセンス情報保持部１４４０と、データバスＢＳ４を介して外部との間でデータ授受を行ない、データバスＢＳ５との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１３５】ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各暗号化コンテンツに対するライセンスをバンクごとに保持する。

【０１３６】なお、図１０において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）である。

【０１３７】もちろん、メモリ１４１５も含めて、モジュールＴＲＭ内に組込まれる構成としてもよい。しかしながら、図１０に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

【０１３８】次に、図１に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【０１３９】図１１および図１２は、図１に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１および第２のフローチャートである。

【０１４０】図１１および図１２においては、携帯電話ユーザが、メモリカード１１０を用いることで、携帯電話機１００を介して配信サーバ３０から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【０１４１】まず、携帯電話ユーザの携帯電話機１００から、携帯電話ユーザによるキー操作部１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【０１４２】そうすると、携帯電話機１００のＭＣＵ１１０６は、配信リクエストがなされたことをバスＢＳ３および結合端子１２２４を介してデータ端末装置１２０のＭＣＵ１２２２へ出力する。そして、ＭＣＵ１２２２は、配信リクエストをメモリインタフェース１２００を介してメモリカード１１０へ出力する。メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａが出力される（ステップＳ１０２）。

【０１４３】データ端末装置１２０は、メモリカード１１０から受理した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを結合端子１２２４およびバスＢＳ３を介して携帯電話機１００へ出力する。携帯電話機１００は、メモリカード１１０からの認証のための認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

【０１４４】配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａ、ライセンス購入条件データＡＣを受信し（ステップＳ１０６）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰｍａで復号処理を実行する（ステップＳ１０８）。

【０１４５】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍｃ１と証明書Ｃｍｃ１を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１０）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を承認し、受理する。そして、次の処理（ステップＳ１１２）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を受理しないで処理を終了する（ステップＳ１７０）。

【０１４６】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍｃ１が禁止クラスリストＣＲＬ

にリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

【０１４７】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

【０１４８】認証の結果、正当な認証データを持つメモリカードを備えるリモコンおよび携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ１によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

【０１４９】暗号化されたセッションキーＫｓ１は、｛Ｋｓ１｝Ｋｍｃ１として、データバスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

【０１５０】携帯電話機１００が、暗号化されたセッションキー｛Ｋｓ１｝Ｋｍｃ１を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ４に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ１により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１２０）。

【０１５１】コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

【０１５２】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストの状態（バージョン）に関連する情報として、リストのバージョンデータＣＲＬ＿ｖｅｒをメモリ１４１５から抽出してデータバスＢＳ５に出力する。

【０１５３】暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍ１および禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１をデータバスＢＳ４に出力する（ステップＳ１２２）。

【０１５４】データバスＢＳ４に出力された暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１は、データバスＢＳ４から端子１２０１およびメモリインタフェース１２００を介してデータ端末装置１２０に出力され、データ端末装置１２０から結合端子１２２４およびバスＢＳ３を介して携帯電話機１００へ出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

【０１５５】配信サーバ３０は、暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍ１およびメモリカード１１０における禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを受理する（ステップＳ１２６）。

【０１５６】禁止クラスリストのバージョン情報ＣＲＬ＿ｖｅｒは、データバスＢＳ１を介して配信制御部３１５に送られ、配信制御部３１５は、受理したバージョンデータＣＲＬ＿ｖｅｒに従って、当該ＣＲＬ＿ｖｅｒのバージョンとＣＲＬデータベース３０６内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データＣＲＬ＿ｄａｔを生成する（ステップＳ１２８）。

【０１５７】さらに、配線制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件データＡＣに従って、ライセンスＩＤ、アクセス制限情報ＡＣ１および再生回路制御情報ＡＣ２を生成する（ステップＳ１３０）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１３２）。

【０１５８】図１２を参照して、配信制御部３１５は、生成したライセンス、すなわち、ライセンス鍵Ｋｃ、再生回路制御情報ＡＣ２、ライセンスＩＤ、コンテンツＩＤ、およびアクセス制限情報ＡＣ１を暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ１によってライセンスを暗号化する（ステップＳ１３６）。暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がデータバスＢＳ１を介して供給する禁止クラスリストの差分データＣＲＬ＿ｄａｔとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、データバスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

【０１５９】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向

上させることができる。

【０１６０】携帯電話機１００は、送信された暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ２を受信し（ステップＳ１４０）、ＭＣＵ１１０６は、バスＢＳ３および結合端子１２２４を介して暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ２をデータ端末装置１２０へ出力する。そして、データ端末装置１２０のＭＣＵ１２２２は、メモリインタフェース１２００を介して暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ２をメモリカード１１０へ出力する。メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ４に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてデータバスＢＳ４の受信データを復号しデータバスＢＳ５に出力する（ステップＳ１４２）。

【０１６１】この段階で、データバスＢＳ５には、Ｋｍ１保持部１４２１に保持される秘密復号鍵Ｋｍ１で復号可能な暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１と、ＣＲＬ＿ｄａｔとが出力される。コントローラ１４２０の指示によって、暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１は、復号処理部１４２２において、秘密復号鍵Ｋｍ１によって復号されたライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤおよび再生回数制限ＡＣ１および再生期限ＡＣ２）が受理され、ライセンス情報保持部１４４０に記録される（ステップＳ１４６）。

【０１６２】コントローラ１４２０は、受理したＣＲＬ＿ｄａｔに基づいて、メモリ１４１５内の禁止クラスリストデータＣＲＬおよびそのバージョンを更新する（ステップＳ１４８）。

【０１６３】ステップＳ１４８までの処理がメモリカード１１０で正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ１５２）。

【０１６４】配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを取得して、これらのデータをデータバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１５４）。

【０１６５】携帯電話機１００は、｛Ｄａｔａ｝Ｋｃ／／Ｄａｔａ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを受理する（ステップＳ１５６）。暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆは、バスＢＳ３、結合端子１２２４、およびメモリインタフェース１２００を介してメモリカード１１０のデータバスＢＳ４に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆがそのままメモリ１４１５に記録される（ステップＳ１５８）。

【０１６６】さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ１６０）、配信サーバ３０で配信受理を受信すると（ステップＳ１６２）、課金データベース３０２への課金データの格納等を伴って、配信終了の処理が実行され（ステップＳ１６４）、全体の処理が終了する（ステップＳ１７０）。

【０１６７】このようにして、携帯電話機１００のデータ端末装置１２０に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍｃ１とともに暗号化して送信できた公開暗号鍵ＫｐｌおよびＫｍｃ１が有効であることを確認した上で、それぞれのクラス証明書Ｃｍｃ１が禁止クラスリスト、すなわち、公開暗号鍵ＫｐｌおよびＫｍｃ１による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１６８】次に、図１３および図１４を参照してメモリカード１１０に配信されたコンテンツデータのデータ端末装置１２０における再生動作について説明する。図１３を参照して、再生動作の開始とともに、携帯電話機１００のユーザからキー操作部１１０８を介して再生指示が携帯電話機１００にインプットされる（ステップＳ２００）。そうすると、ＭＣＵ１１０６は、再生指示をバスＢＳ３および結合端子１２２４を介してＭＣＵ１２２２へ出力する。そして、ＭＣＵ１２２２は、データバスＢＳ３を介して認証データ保持部１２０２から認証データ｛ＫＰｐｌ／／Ｃｒｔｆｌ｝ＫＰｍａを読出し、メモリインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐｌ／／Ｃｒｔｆｌ｝ＫＰｍａを入力する（ステップＳ２０１）。

【０１６９】そうすると、メモリカード１１０は、認証データ｛ＫＰｐｌ／／Ｃｒｔｆｌ｝ＫＰｍａを受理する（ステップＳ２０２）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐｌ／／Ｃｒｔｆｌ｝ＫＰｍａを、ＫＰｍａ保持部１４１４に保持された公開認証鍵ＫＰｍａによって復号し（ステップＳ２０３）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐｌ／／Ｃｒｔｆｌ｝ＫＰｍａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ２０４）。復号できなかった場

合、コントローラ１４２０は認証データ不受理の出力をデータＢＳ４および端子１２０１を介してデータ端末装置１２０のメモリインタフェース１２００へ出力する（ステップＳ２０６）。認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｒｔｆ１がメモリ１４１５から読出した禁止クラスリストデータに含まれるか否かを判断する（ステップＳ２０５）。この場合、証明書Ｃｒｔｆ１にはＩＤが付与されており、コントローラ１４２０は、受理した証明書Ｃｒｔｆ１のＩＤが禁止クラスリストデータの中に存在するか否かを判別する。証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれると判断されると、コントローラ１４２０は認証データ不受理の出力をデータＢＳ４および端子１２０１を介してリモコン１２０のメモリインタフェース１２００へ出力する（ステップＳ２０６）。

【０１７０】ステップＳ２０４において認証データが公開認証鍵ＫＰｍａで復号できなかったとき、およびステップＳ２０５において受理した証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、データ端末装置１２０のＭＣＵ１２２２は、メモリインタフェース１２００を介して認証データ不受理の出力を受けると、その旨をバスＢＳ３および結合端子１２２４を介して携帯電話機１００へ出力する（ステップＳ２０７）。そして、携帯電話機１００のＭＣＵ１１０６は、認証データ不受理のデータをディスプレイ１１１０に表示する（ステップＳ２０７）。

【０１７１】ステップＳ２０５において、証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれていないと判断されると、図１４を参照して、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ２０８）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をデータバスＢＳ４へ出力する（ステップＳ２０９）。そうすると、コントローラ１４２０は、端子１２０１を介してメモリインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力し、データ端末装置１２０のＭＣＵ１２２２は、メモリインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１２０４は、秘密復号鍵Ｋｐ１を復号処理部１２０５へ出力する。

【０１７２】復号処理部１２０５は、Ｋｐ１保持部１２０４から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１２０８へ出力する（ステップＳ２１０）。そうすると、セッションキー発生部１２１０は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１２０８へ出力する（ステップＳ２１１）。暗号処理部１２０８は、セッションキー発生部１２１０からのセッションキーＫｓ３を復号処理部１２０６からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、ＭＣＵ１２２２は、データバスＢＳ３およびメモリインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ２１２）。

【０１７３】メモリカード１１０の復号処理部１４１２は、端子１２０１およびデータバスＢＳ４を介して｛Ｋｓ３｝Ｋｓ２を入力し、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、データ端末装置１２０で発生されたセッションキーＫｓ３を取得する（ステップＳ２１３）。

【０１７４】セッションキーＫｓ３の受理に応じて、コントローラ１４２０は、ライセンス情報保持部１４４０内の対応するアクセス制限情報ＡＣ１を確認する（ステップＳ２１４）。

【０１７５】ステップＳ２１４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数に制限があるが、再生可能な場合には、ライセンス情報保持部１４４０に記録されたアクセス制限情報ＡＣ１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ２１５）。一方、アクセス制限情報ＡＣ１によって再生回数が制限されていない場合においては、ステップＳ２１５はスキップされ、再生制御情報ＡＣ１は更新されることなく処理が次のステップ（ステップＳ２１６）に進行される。

【０１７６】また、ライセンス情報保持部１４４０内にリクエスト曲の当該コンテンツＩＤが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【０１７７】ステップＳ２１４において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部１４４０に記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生回路制御情報ＡＣ２がデータバスＢＳ５上に得られる（ステップＳ２１６）。

【０１７８】得られたライセンス鍵Ｋｃと再生回路制御情報ＡＣ２は、切換スイッチ１４４４の接点Ｐｄを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｄを介して復号処理部１４１２より受けたセッションキーＫｓ３によってデータバスＢＳ５から受けたライセンス鍵Ｋｃと再生回路制御情報ＡＣ２とを暗号化し、｛Ｋｃ／／ＡＣ２｝Ｋｓ３をデータバスＢＳ３に出力する（ステップＳ２１７）。

【０１７９】データバスＢＳ４に出力された暗号化デー

タは、メモリインタフェース１２００を介してデータ端末装置１２０に送出される。

【０１８０】データ端末装置１２０においては、メモリインタフェース１２００を介してデータバスＢＳ３に伝達される暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｓ３を復号処理部１２１２によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生回路制御情報ＡＣ２を受理する（ステップＳ２１８）。復号処理部１２１２は、ライセンス鍵Ｋｃ、および再生回路制御情報ＡＣ２をデータバスＢＳ３に出力する。

【０１８１】ＭＣＵ１２２２は、データバスＢＳ３を介して、再生回路制御情報ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２１９）。

【０１８２】ステップＳ２１９においては、再生回路制御情報ＡＣ２によって再生不可と判断される場合には、再生動作は終了される。

【０１８３】ステップＳ２１９において再生可能と判断された場合、ＭＣＵ１２２２は、メモリインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、データバスＢＳ４および端子１２０１を介してメモリインタフェース１２００へ出力する（ステップＳ２２０）。

【０１８４】データ端末装置１２０のＭＣＵ１２２２は、メモリインタフェース１２００を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、データバスＢＳ３を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１４へ与える。また、ＭＣＵ１２２２は、復号処理部１２１２から出力されたバスＢＳ３上のコンテンツ鍵Ｋｃを復号処理部１２１４へ与える。

【０１８５】そして、復号処理部１２１４は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ２２１）。

【０１８６】そして、復号されたコンテンツデータＤａｔａはＭＰ３デコーダ１２１６へ出力され、ＭＰ３デコーダ１２１６は、コンテンツデータを解凍して再生し、ＤＡＣ１２１８はディジタル信号をアナログ信号に変換してジャック１２２０へ出力する。そして、音楽データはジャック１２２０を介してヘッドホン１３０へ出力されて再生される（ステップＳ２２２）。これによって再生動作が終了する。

【０１８７】上述したように、データ端末装置１２０を含むアダプタ１４０を用いることにより、暗号化音楽データを配信サーバ３０からメモリカード１１０へダウンロードし、そのダウンロードした暗号化音楽データを復号して再生できる。

【０１８８】また、アダプタ１４０を携帯電話機に装着することによって、データ端末装置１２０の機能を必要とするユーザはアダプタ１４０を追加購入すれば、暗号化音楽データを配信サーバ３０からメモリカード１１０へダウンロードし、そのダウンロードした暗号化音楽データを復号して再生できる。

【０１８９】［実施の形態２］この発明による携帯電話機は、図１５に示す携帯電話機１００Ａであっても良い。携帯電話機１００Ａは、図３に示す携帯電話機１００の本体１０５を本体１０５Ａに代え、アダプタ１４０をアダプタ１４０Ａに代えたものであり、その他は携帯電話機１００と同じである。本体１０５Ａは、携帯電話機１００の本体１０５にバッテリ１５０を追加したものであり、その他は本体１０５と同じである。また、アダプタ１４０Ａは、アダプタ１４０からバッテリ１５０を削除したものであり、その他はアダプタ１４０と同じである。

【０１９０】バッテリ１５０は、ＭＣＵ１１０６、および音声コーデック１１１２に駆動電力を供給するとともに、結合端子１１１８を介してアダプタ１４０Ａのデータ端末装置１２０にも駆動電力を供給する。

【０１９１】携帯電話機１００Ａを用いても、実施の形態１において説明したのと同じ方法によって配信サーバ３０からメモリカード１１０へ暗号化音楽データをダウンロードできるとともに、メモリカード１１０から暗号化音楽データを読出し、復号および再生を行なうことができる。

【０１９２】携帯電話機１００Ａは、バッテリ１５０が本体１０５Ａの駆動電力と、データ端末装置１２０の駆動電力とを賄なうことができる容量を持っている場合、アダプタ１４０Ａのみを購入すれば、暗号化音楽データのダウンロードおよび復号・再生を行なうことができる。したがって、携帯電話機１００Ａのユーザはアダプタ１４０Ａだけを購入し、自己の携帯電話機にアダプタ１４０Ａを装着することによって携帯電話機１００Ａを用いて、暗号化音楽データをダウンロードし、その暗号化音楽データを再生して聴くことができる。本実施の形態２においてはバッテリ１５０を本体１０５Ｃに備えるように説明したが、バッテリ１５０は本体１０５Ｃにコネクタ等で接続されていて、本体１０５Ｃから着脱可能な構造としてもよい。

【０１９３】［実施の形態３］この発明による携帯電話機は、図１６に示す携帯電話機１００Ｂであっても良い。携帯電話機１００Ｂは、図３に示す携帯電話機１００の本体１０５を本体１０５Ｂに代え、アダプタ１４０をアダプタ１４０Ｂに代えたものであり、その他は携帯電話機１００と同じである。本体１０５Ｂは、携帯電話機１００の本体１０５に混合回路１１２４を追加し、ジャック１１１４をジャック１１２２に代えたものであり、その他は本体１０５と同じである。また、アダプタ１４０Ｂは、携帯電話機１００のアダプタ１４０からジ

ャック１２２０を削除したものであり、その他はアダプタ１４０と同じである。

【０１９４】混合回路１１２４は、音声コーデック１１１２によって復調およびディジタル信号からアナログ信号への変換が行われた音声データをジャック１１２２へ出力する。また、混合回路１１２４は、アダプタ１４０Ｂのデータ端末装置１２０によって復号および再生が行なわれた音楽データを結合端子１１２０を介して受取り、その受取った音楽データをジャック１１２２へ出力する。

【０１９５】ジャック１１２２は、混合回路１１２４からの音声データまたは音楽データをヘッドホン１３０へ出力する。また、ジャック１１２２は、携帯電話機１００Ｂのユーザが話した音声データをマイク（図示せず）を介して受取り、音声コーデック１１１２へ出力する。なお、ジャック１１２２は、マイクからの音声データを入力し、２チャンネルの音楽データまたは音声データをヘッドホン１３０へ出力するため、４芯のジャックとなっている。また、１つのジャックを介して音声データを入出力し、音楽データを出力するので、携帯電話機による通常の通話を行ないながら、音楽を聴くことができる。その他は、実施の形態１の説明と同じである。

【０１９６】携帯電話機１００Ｂを用いても、実施の形態１において説明したのと同じ方法によって配信サーバ３０からメモリカード１１０へ暗号化音楽データをダウンロードできるとともに、メモリカード１１０から暗号化音楽データを読出し、復号および再生を行なうことができる。

【０１９７】［実施の形態４］この発明による携帯電話機は、図１７に示す携帯電話機１００Ｃであっても良い。携帯電話機１００Ｃは、図１６に示す携帯電話機１００Ｂの本体１０５Ｂを本体１０５Ｃに代え、アダプタ１４０Ｂをアダプタ１４０Ｃに代えたものであり、その他は携帯電話機１００Ｂと同じである。本体１０５Ｃは、携帯電話機１００Ｂの本体１０５Ｂにバッテリ１５０を追加したものであり、その他は本体１０５Ｂと同じである。また、アダプタ１４０Ｃは、アダプタ１４０Ｂからバッテリ１５０を削除したものであり、その他はアダプタ１４０Ｂと同じである。

【０１９８】バッテリ１５０は、ＭＣＵ１１０６、音声コーデック１１１２、および混合回路１１２４に駆動電力を供給するとともに、結合端子１１１８を介してアダプタ１４０Ｃのデータ端末装置１２０にも駆動電力を供給する。

【０１９９】携帯電話機１００Ｃを用いても、実施の形態１において説明したのと同じ方法によって配信サーバ３０からメモリカード１１０へ暗号化音楽データをダウンロードできるとともに、メモリカード１１０から暗号化音楽データを読出し、復号および再生を行なうことができる。

【０２００】携帯電話機１００Ｃは、バッテリ１５０が本体１０５Ｃの駆動電力と、データ端末装置１２０の駆動電力とを賄なうことができる容量を持っている場合、アダプタ１４０Ｃのみを購入すれば、暗号化音楽データのダウンロードおよび復号・再生を行なうことができる。そして、携帯電話機１００Ｃのユーザは１つのジャック１１２２を介して通常の電話機能による音声データと、音楽データをステレオによって聴くことができる。その他は、実施の形態１，３と同じである。

【０２０１】本実施の形態においてはバッテリ１５０を本体１０５Ｃに備えるように説明したが、バッテリ１５０は本体１０５Ｃにコネクタ等で接続されていて、本体１０５Ｃから着脱可能な構造としてもよい。

【０２０２】また、実施の形態１～４において、アダプタ１４０には暗号化コンテンツデータまたはライセンスの配信を受け、暗号化コンテンツデータを再生するデータ端末装置１２０を備えるように説明したが、必ずしも両機能を備える必要はなく、配信を受ける機能と暗号化コンテンツデータを再生する機能のいずれか一つのみを行なうデータ端末装置を備えるものであってもよい。

【０２０３】さらに、実施の形態１～４において、ＭＰ３方式によって符号化された音楽データを扱うように説明したが、特に、ＭＰ３に限定するものではなく、音楽が生成可能なディジタルデータであればいかなる符号化方式によって符号化された音楽データであってもよい。

【０２０４】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　本発明による携帯電話機の裏面の平面図である。

【図３】　実施の形態１による携帯電話機の概略ブロック図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図６】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

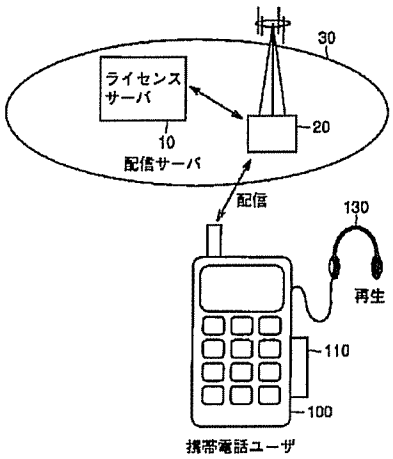
【図７】　ライセンスサーバの構成を示す概略ブロック図である。

【図８】　実施の形態１における携帯電話機の構成を示すブロック図である。

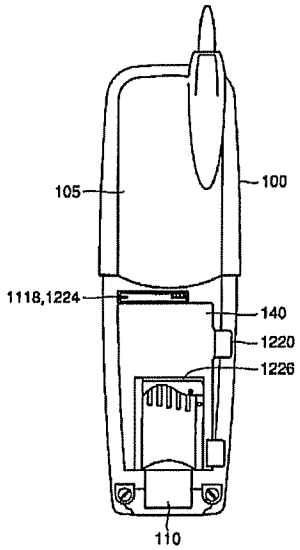
【図９】　図３に示す携帯電話機に含まれるデータ端末装置の構成を示すブロック図である。

【図１０】　実施の形態１におけるメモリカードの構成を示すブロック図である。
【図１１】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。
【図１２】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。
【図１３】　実施の形態１における携帯電話機における再生動作を説明するための第１のフローチャートである。
【図１４】　実施の形態１における携帯電話機における再生動作を説明するための第２のフローチャートである。
【図１５】　実施の形態２における携帯電話機の構成を示すブロック図である。
【図１６】　実施の形態３における携帯電話機の構成を示すブロック図である。
【図１７】　実施の形態４における携帯電話機の構成を示すブロック図である。
【符号の説明】
１０　ライセンスサーバ、２０　配信キャリア、３０　配信サーバ、１００，１００Ａ，１００Ｂ，１００Ｃ　携帯電話機、１０５，１０５Ａ，１０５Ｂ，１０５Ｃ　本体、１１０　メモリカード、１２０　データ端末装置、１３０　ヘッドホン、１４０，１４０Ａ，１５４０＊Ｂ，１４０Ｃ　アダプタ、１５０　バッテリ、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３１０　データ処理部、３１２，３２０，１２０５，１２１２，１４０４，１４０８，１４１２，１４２２　復号処理部、３１５　配信制御部、３１６，１２１０，１４１８　セッションキー発生部、３１８，３２６，３２８，１２０８，１４０６，１４１０　暗号処理部、３５０　通信装置、１１０２　アンテナ、１１０４　送受信部、１１０６，１２２２　MCU、１１０８　キー操作部、１１１０　ディスプレイ、１１１１　スピーカ、１１１２　音声コーデック、１１１３　マイク、１２１８　DAC、１１１４，１２２０　ジャック、１２０１　端子、１１１６　バッド、１１１８，１２２４　結合端子、１１２４混合回路、１２００　メモリインタフェース、１２０２，１４００　認証データ保持部、１２０４　Ｋｐ１保持部、１２０６　公開復号部、１２１４　ＤＥＳ、１２１６　ＭＰ３デコーダ、１２２６　着脱部、１２３０　共通鍵暗号・復号部、１４０２　Ｋｍｃ１保持部、１４１４　ＫＰｍａ保持部、１４１５　メモリ、１４１６　ＫＰｍ１保持部、１４２０　コントローラ、１４２１　Ｋｍ１保持部、１４４０　ライセンス情報保持部、１４４２，１４４４，１４４６　切換スイッチ。

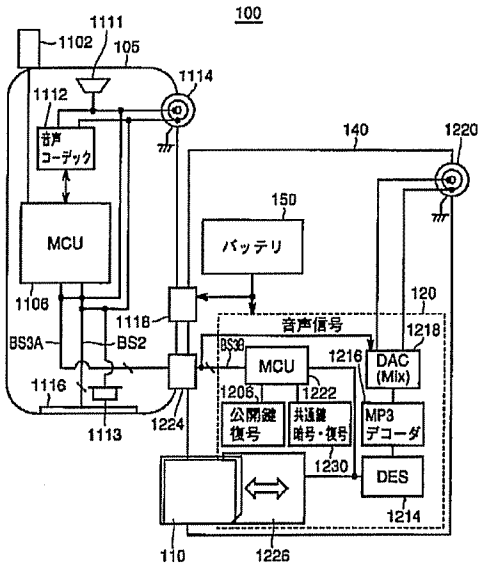
【図１】



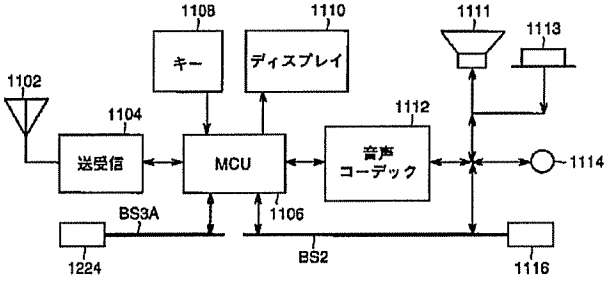
【図２】



【図３】



【図８】



【図４】

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	音楽データ
Kc	ライセンス鍵		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。
Data-Inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可）
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報（例：再生可否）

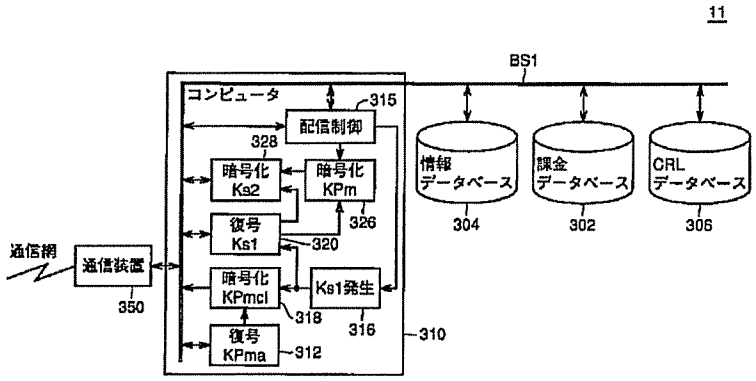
【図６】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		データ端末装置	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵（非対称鍵）	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

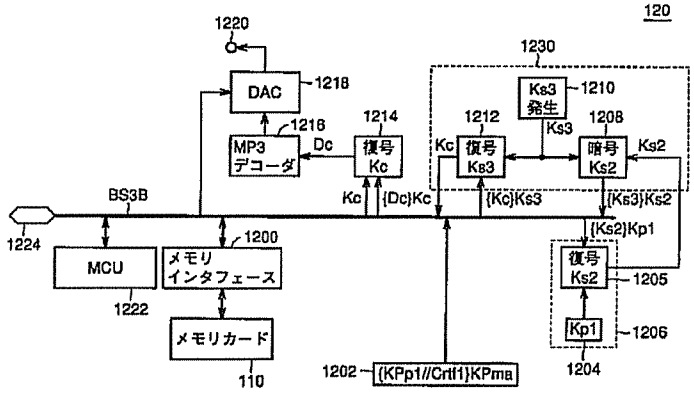
【図５】

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 （差分データ形式）
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 （非対称鍵）	データ端末装置	Kpnにて復号可能。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊データ端末装置の種類nごとに異なる。
KPmcl	公開暗号鍵 （非対称鍵）	メモリカード	Kmclにて復号可能。 {KPmcl//Cmcl}KPmaの形式で出荷時に記録 ＊メモリカードの種類ごとに異なる。
Kpn	秘密復号鍵	データ端末装置	コンテンツ再生回路（データ端末装置）固有の復号鍵 ＊データ端末装置の種類nごとに異なる。
Kmcl	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ＊メモリカードの種類ごとに異なる。
Crtfn	クラス証明書	データ端末装置	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊データ端末装置のクラスnごとに異なる。
Cmcl		メモリカード	メモリカードのクラス証明書。認証機能を有する。 {KPmcl//Cmcl}KPmaの形式で出荷時に記録 ＊メモリカードのクラスlごとに異なる。

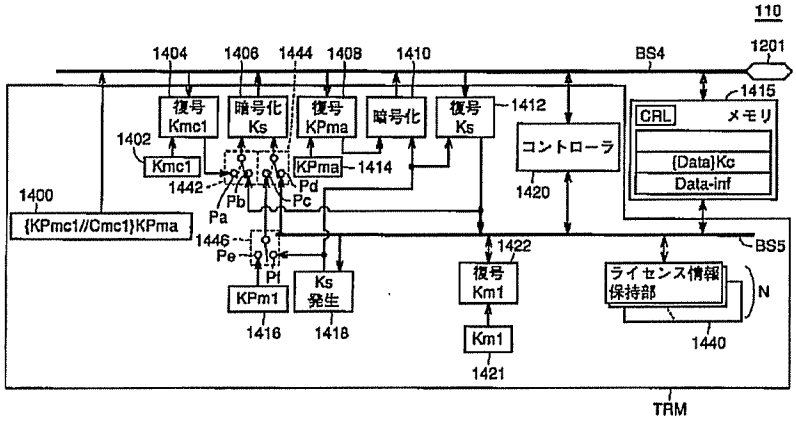
【図７】



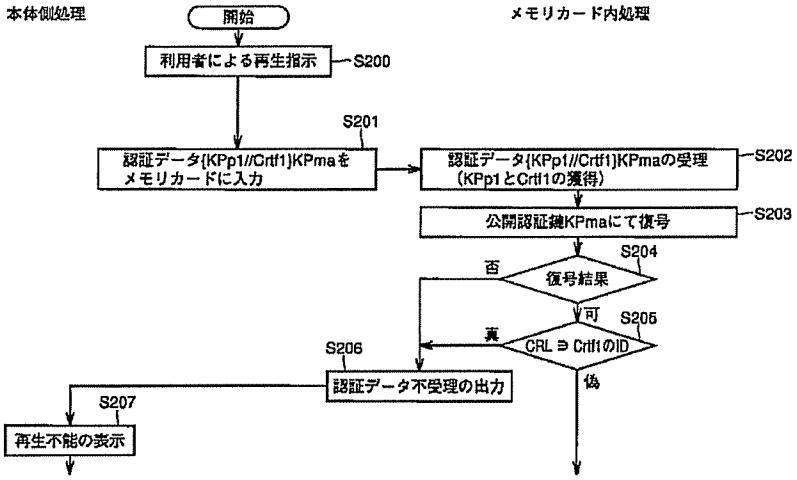
【図９】



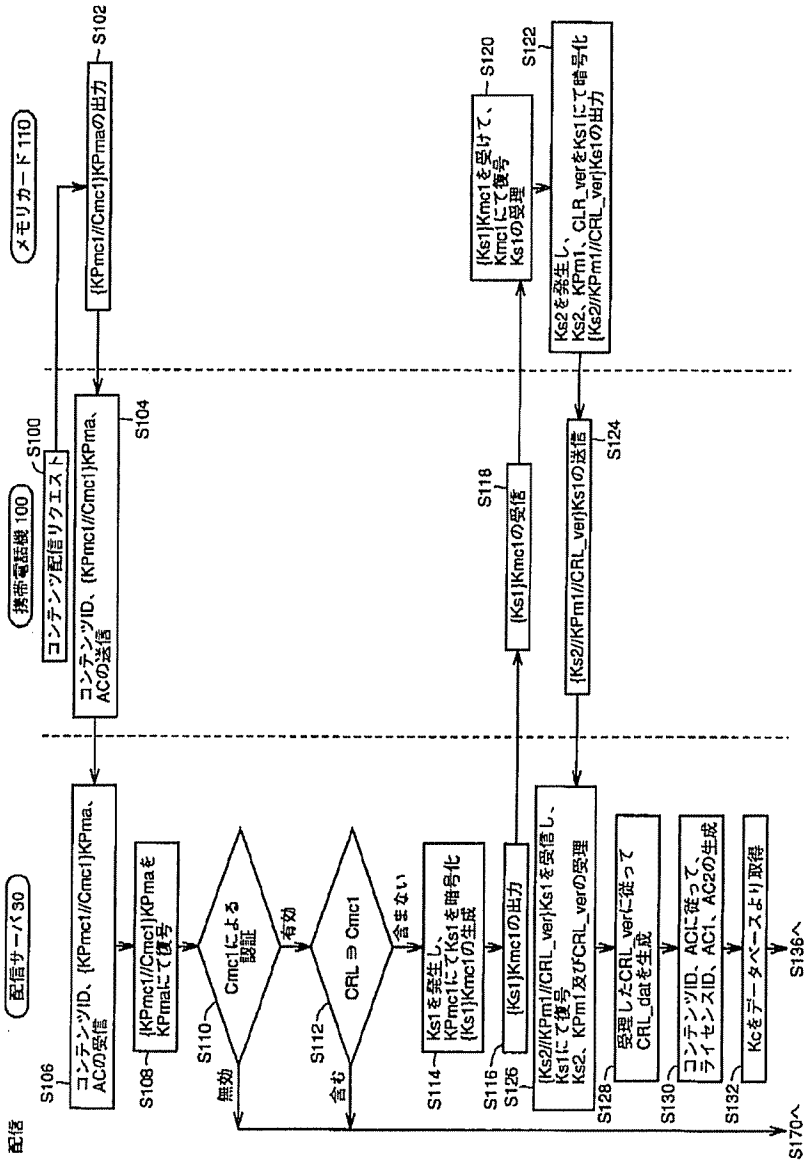
【図１０】


110
1404
1406
1444
1408
1410
BS4
1201
1415
CRL
メモリ
{Data}Kc
Data-inf
復号 Kmc1
暗号化 Ks
復号 KPma
暗号化
復号 Ks
1412
コントローラ
1420
1402
Kmc1
KPma
1414
1442
Pb
Pd
Pc
Pa
1400
{KPmc1//Cmc1}KPma
1446
Pe
Pf
BS5
1422
復号 Km1
ライセンス情報保持部
N
KPm1
Ks 発生
1416
1418
Km1
1421
1440
TRM

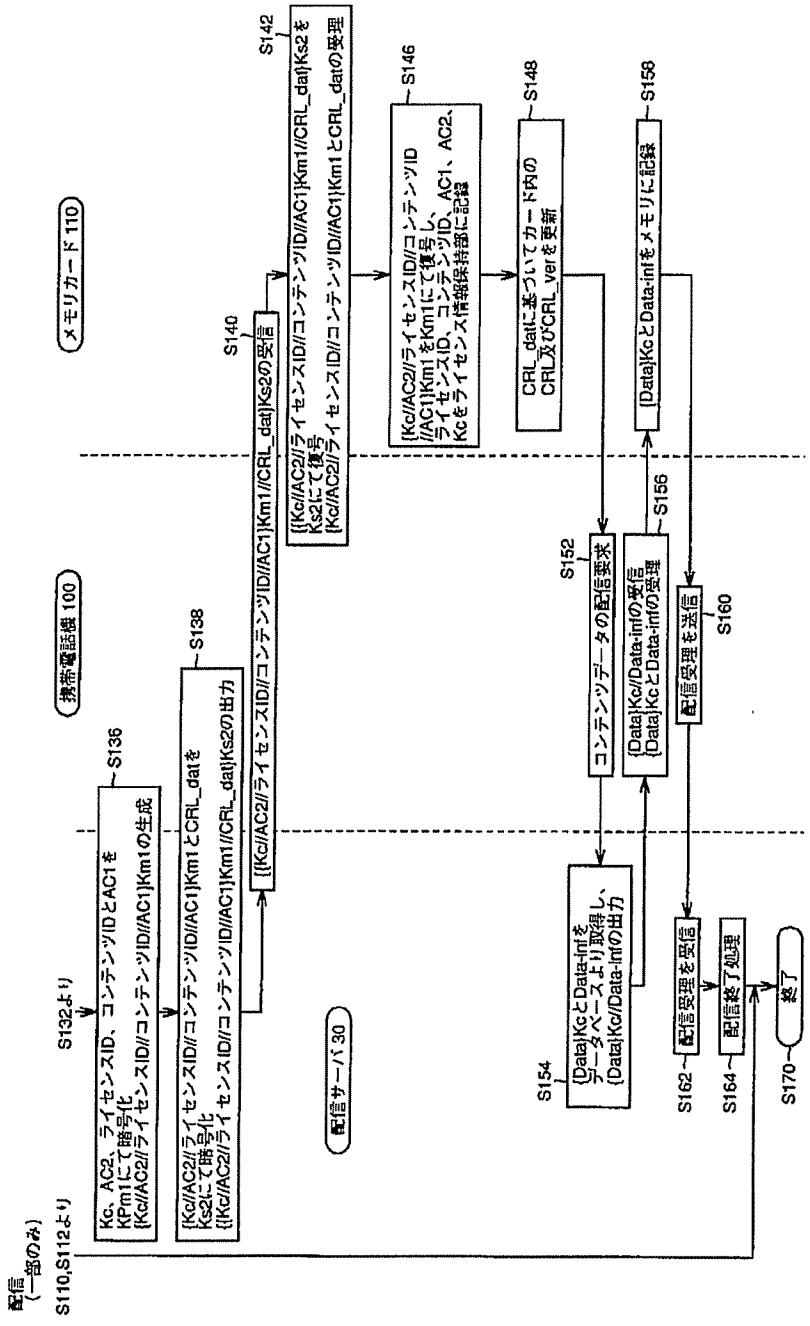
【図１３】


本体側処理
開始
利用者による再生指示
S200
S201
認証データ{KPp1//Crtf1}KPmaを メモリカードに入力
認証データ{KPp1//Crtf1}KPmaの受理 (KPp1とCrtf1の獲得)
S202
公開認証鍵KPmaにて復号
S203
S204
否
復号結果
可
S205
真
CRL ∋ Crtf1のID
S206
認証データ不受理の出力
偽
S207
再生不能の表示
メモリカード内処理

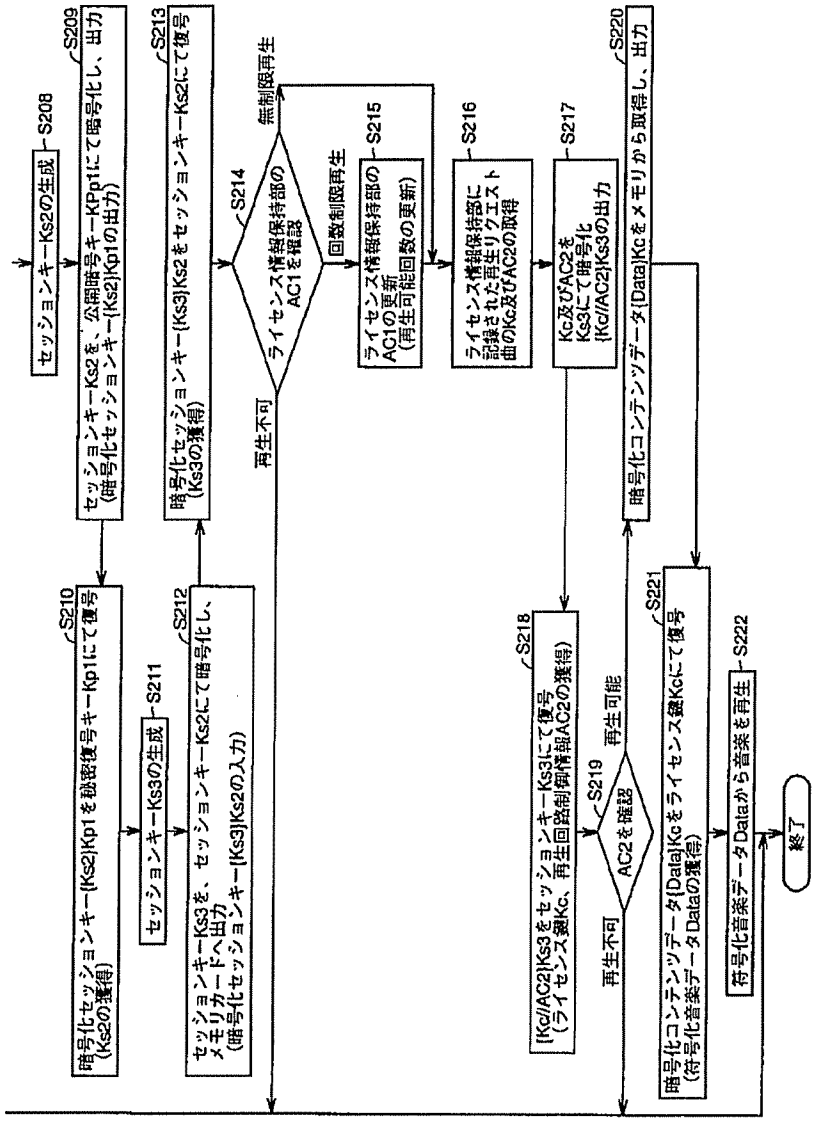
【図１１】


メモリカード 110
携帯電話機 100
配信サーバ 30
配信
S100
コンテンツ配信リクエスト
S102
{KPmc1//Cmc1}KPmaの出力
コンテンツID、{KPmc1//Cmc1}KPma、ACの送信
S104
S106
コンテンツID、{KPmc1//Cmc1}KPma、ACの受信
S108
{KPmc1//Cmc1}KPmaをKPmaにて復号
S110
Cmc1による認証
無効
有効
S112
CRL ∋ Cmc1
含む
含まない
S114
Ks1を発生し、KPmc1にてKs1を暗号化{Ks1}Kmc1の生成
S116
{Ks1}Kmc1の出力
S118
{Ks1}Kmc1の受信
S120
{Ks1}Kmc1を受けて、Kmc1にて復号Ks1の受理
S122
Ks2を発生し、Ks2、KPm1、CLR_verをKs1にて暗号化{Ks2//KPm1//CRL_ver}Ks1の出力
S124
{Ks2//KPm1//CRL_ver}Ks1の送信
S126
{Ks2//KPm1//CRL_ver}Ks1を受信し、Ks1にて復号Ks2、KPm1及びCRL_verの受理
S128
受理したCRL_verに従ってCRL_datを生成
S130
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S132
Kcをデータベースより取得
S136へ
S170へ

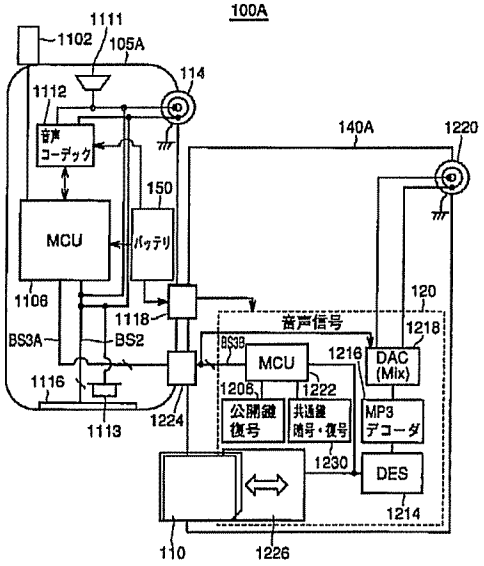
【図１２】


メモリカード110
携帯電話機100
配信サーバ30
配信
（一部のみ）
S110,S112より
S132より
S136
Kc、AC2、ライセンスID、コンテンツIDとAC1を
KPm1にて暗号化
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1の生成
S138
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datを
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の出力
S140
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受信
S142
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datの受理
S146
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をKm1にて復号し、
ライセンスID、コンテンツID、AC1、AC2、
Kcをライセンス情報保持部に記録
S148
CRL_datに基づいてカード内の
CRL及びCRL_verを更新
S152
コンテンツデータの配信要求
S154
{Data}KcとData-infを
データベースより取得し、
{Data}Kc//Data-infの出力
S156
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S158
{Data}KcとData-infをメモリに記録
S160
配信受理を送信
S162
配信受理を受信
S164
配信終了処理
S170
終了

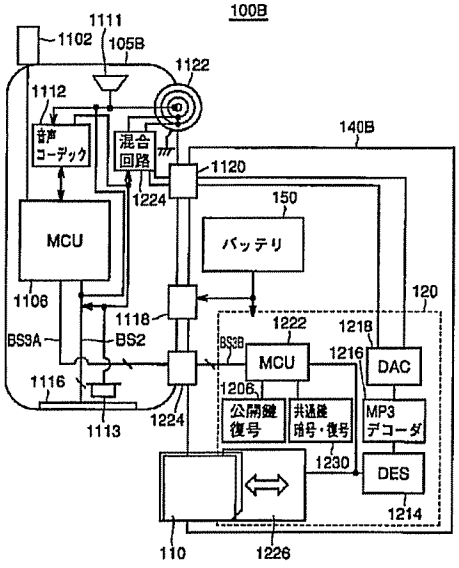
【図１４】


セッションキーKs2の生成
S208
セッションキーKs2を、公開暗号キーKPp1にて暗号化し、出力
(暗号化セッションキー{Ks2}Kp1の出力)
S209
暗号化セッションキー{Ks2}Kp1にて復号
(Ks2の獲得)
S210
セッションキーKs3の生成
S211
セッションキーKs3を、セッションキーKs2にて暗号化し、メモリカードへ出力
(暗号化セッションキー{Ks3}Ks2の入力)
S212
暗号化セッションキー{Ks3}Ks2をセッションキーKs2にて復号
(Ks3の獲得)
S213
ライセンス情報保持部のAC1を確認
S214
無制限再生
回数制限再生
再生不可
ライセンス情報保持部のAC1の更新
(再生可能回数の更新)
S215
ライセンス情報保持部に記録された再生リクエスト曲のKc及びAC2の取得
S216
Kc及びAC2をKs3にて暗号化{Kc//AC2}Ks3の出力
S217
暗号化コンテンツデータ{Data}Kcをメモリから取得し、出力
S220
{Kc//AC2}Ks3をセッションキーKs3にて復号
(ライセンス鍵Kc、再生回路制御情報AC2の獲得)
S218
AC2を確認
S219
再生可能
再生不可
暗号化コンテンツデータ{Data}Kcをライセンス鍵Kcにて復号
(符号化音楽データDataの獲得)
S221
符号化音楽データDataから音楽を再生
S222
終了

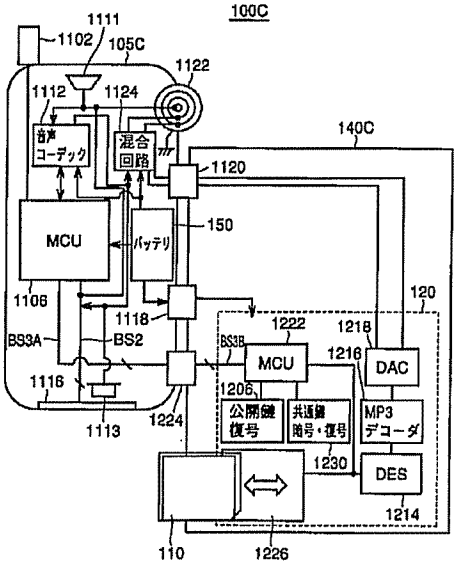
【図１５】



【図１６】



【図１７】



フロントページの続き

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	9/32		H04M	11/00	302
H04M	1/00		G10L	9/00	N
	1/02		H04B	7/26	M
	1/725		H04L	9/00	601B
	11/00	302			601E

Ｆターム(参考) 5J104 AA07 AA16 EA06 EA19 EA22
KA02 KA05 NA03 NA35 NA37
NA41 NA42 NA43 PA02
5K023 AA07 MM21 PP01 PP11
5K027 AA11 FF01 FF25 HH26
5K067 AA32 BB04 DD54 DD57 EE02
EE10 EE16 FF26 FF40 HH07
HH23 HH36 KK05 KK15
5K101 KK18 LL12 NN01 NN15 NN21